

Privacy Impact Assessment - 2008 (Form) / One VA Contact Management-2008 (Item)

ProSight

PIA 2008 SECTIONS 1 - 4

INTRODUCTION:

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person. Appendix A, "Applicable Legal and Regulatory Requirements" summarizes the applicable legal and regulatory requirements that are addressed by the PIA process.

Update regarding PIV projects: Federal Information Processing Standards Publication (FIPS PUB) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors and subsequent OMB guidance explicitly require PIAs for PIV projects collecting any personal data, not just of the public.

Primary Privacy Impact Assessment objectives include:

- o Ensure and promote the trust and confidence of Veterans and the general public.
- o Ensure compliance with the eGov Act and other applicable privacy laws, regulations and policies, including the PIV regulations.
- o Identify the risks and adverse effects of collecting, maintaining and disseminating personal information in electronic information systems.
- o Evaluate and develop protections and alternative processes for handling information to mitigate potential privacy risks.

Additional important objectives include:

- o Provide a mechanism for ensuring responsibility and accountability for privacy issues.
- o Provide documented assurance that privacy, security and other vital data stewardship considerations are integrated into information technology systems, starting with the initial outlining of a project's objectives and data usage requirements and continuing through design, operation, maintenance and disposal.
- o Ensure that decision-makers are provided the information required to make informed system design or procurement decisions, based on an understanding of privacy risk, and of options available for mitigating that risk.
- o Greatly reduce the risk of needing to interrupt a program or service because privacy and other vital data stewardship considerations were not adequately addressed before the program or service was implemented.
- o Promote awareness and understanding of privacy issues.
- o Provide valuable documentation on the flow of personal information, and related privacy considerations and design decisions.

Completion of this PIA Form:

- o Part I (Sections 1 and 2) of this form must be completed for all projects. Part I documents basic project information and establish whether a full PIA is required.
- o This entire PIA Form (Parts I and II) must be completed/updated every year for all projects with information technology (IT) systems that collect, maintain, and/or disseminate "personally identifiable information" information that may be used to identify a specific person of the public, OR is a PIV project.

Important Note: While this form provides detailed instructions for completing a Privacy Impact Assessment for your project, support documents that provide additional guidance are available on the OCIS Portal (VA network access required).

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

One VA Contact Management-2008

1.1.b) OMB Unique Project Identifier:

029-00-02-00-01-1026-00-305-108

1.1.c) Concise Project Description

Provide a concise description of the project. Your response will be automatically limited to approximately 200 words, and should provide a basic understanding of the project, and its most essential elements. (If applicable, use of personal data is to be described in Section 3.)

CM will provide the business driven requirements that will drive the design and development of solutions supporting Contact Management across all channels including personal interviews, telephones, postal mail (USPS), E-mail, and Internet services--such as Frequently Asked Question Boards and web portals-- internment services, and interactions with private industry partners. CM will identify the business requirements for providing centralized knowledge and data management systems providing for consolidated One-VA information environment used by constituents and employees alike. CM will implement the benchmarking standards for assessing and continually improving VA's customer service.

1.1.d) Additional Project Information (Optional)

The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.

In order to achieve the envisioned success of Contact Management, the Contact Management Strategy Team is comprised of Administration representatives grouped into four sub-initiatives called Integrated Project Teams (IPTs):

1. Benefit Self-Service and Enhanced Access—To provide self-service opportunities that allow 24/7 interaction with VA. Enhance the ability of a veteran, beneficiaries, or any business partner to access information, apply for benefits, and conduct self- service activities across the benefit lifecycle through the OneVA Portal. This IPT is shared with the Registration and Eligibility initiative.
2. Contact Centers— To optimize telephony, email interaction capability and improve customer service by reducing call blockage and drop rates, maximizing first time contact resolution, and offering self-service options.
3. Knowledge Management System--To improve the accuracy, consistency, and timeliness of answers provided to veterans and customers of VA through shared data and knowledge management. This system will allow employees access to up-to-date information for all Lines of Business in order to provide consistent answers and allow resolution of inquiries correctly the first time resulting in increased efficiency, productivity, and customer satisfaction.
4. OneVA Portal--To provide a OneVA delivery vehicle for self service solutions, centralize stakeholder access to VA online services and content, improve online services and content by leveraging the functionality available through web portal technology, and provide a single, consistent, seamless information delivery channel for veterans, beneficiaries, employees, and business partners.

1.2) Contact Information:

1.2.a) Person completing this document:	
Title:	Evangelina Dobbs, PMP, Contractor
Organization:	005E1
Telephone Number:	202-272-9494
Email Address:	evangelina.dobbs@va.gov
1.2.b) Project Manager:	
Title:	Rebecca Wells
Organization:	Enterprise Architecture (005E1)
Telephone Number:	202-357-3953

Email Address:	rebecca.wells@va.gov
1.2.c) Staff Contact Person:	
Title:	Rebecca Wells
Organization:	005E1
Telephone Number:	202-357-3953
Email Address:	rebecca.wells@va.gov

ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.

Currently, the CM strategy teams are planning, strategizing and developing requirements. After cost-benefit analyses and guidance from the Executive Oversight Committee, Contact Management projects/deliverables will be deployed in phases. The first phase will be geared toward benefiting the veteran, the second phase toward VA's business partners (e.g., lending institutions, funeral home directors, school officials), and the third phase will concentrate on internal users. Building of the agreed upon products will begin in FY '07 and be finished and deployed in FY '08.

2. DETERMINATION OF PIA REQUIREMENTS:
<i>A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.</i>
2.a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?
Yes
2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?
No
<i>If "YES" to either question then a PIA is required for this project. Complete the remaining questions on this form. If "NO" to both questions then no PIA is required for this project. Skip to section 14 and affirm.</i>
<i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i>

Part II. Privacy Impact Assessment
3. PROJECT DESCRIPTION:
<i>Enter the information requested to describe the project.</i>
3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.
The CM project will access the following information regarding veterans: complete name, address, telephone number, social security number; date of birth, place of birth, and military service history to support VA delivery of service to Veterans including determining eligibility for benefits. This is being determined as part of the requirements definition

phase. The CM Knowledge Management system will not keep personal information – this system will provide business knowledge. All personal (privacy) information will come from VADIR or other benefits processing systems. The information will be provided to veterans via the portal (which will required IDM and authentication) through self-service applications
3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?
Title 38, United States Code, section 210(c) and Chapters 11, 13, 15, 31, 34, 35, and 36.
3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.
More than 20,000,000
3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.
(1) Design/Planning
3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.
Target completion date is September, 2008.
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)
This initiative is directed by Congressional mandate and is part of the President's Management Agenda and the VA's Strategic Plan.

4. SYSTEM OF RECORDS:
<i>The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.</i>
4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?
If "No" then skip to section 5, 'Data Collection'.
Yes
4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?
IF "No" then SKIP to question 4.c.
Yes
4.b.1) For each applicable System of Records, list:
(1) The System of Records identifier (number),
Because this system is the planning phase, the specific SORN has not yet finalized, however the system is likely to be covered by 58VA21/22/28
(2) The name of the System of Records, and
58VA21/22/28 is titled Compensation, Pension, Education, and Rehabilitation Records-VA
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
http://www.va.gov/oit/cio/foia/Privacy/SystemsOfRecords/58VA21.asp
IMPORTANT: For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.
4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?

Yes
4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?
Created for another project or system
If created for another project or system, briefly identify the other project or system.
This system of records was created to cover compensation, pension, education, and rehabilitation records required to be maintained by the VA to provide benefits and confirm eligibility.
4.b.4) Does the System of Records Notice require modification?
If "No" then skip to section 5, 'Data Collection'.
Modification of the System of Records is NOT Required.
4.b.5) Describe the required modifications.
4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.
Explanation:
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIA 2008 SECTION 5

Project Name

One VA Contact Management-2008

5. DATA COLLECTION:

5.1 Data Types and Data Uses

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.

Important Note: Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."

Yes

Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)

Specifically identify the personal information collected, and describe the intended use of the information.

Veteran name, address, telephone number, social security number and military history data will be used by VA caseworkers and/or VA business lines to identify veterans and communicate with veterans regarding benefits and eligibility determinations.

Yes

Other Personal Information of the Veteran or Primary Subject

Specifically identify the personal information collected, and describe the intended use of the information.

Business specific information such as medical, insurance, home loan, education, etc to provide benefits and confirm eligibility. Actual data is TBD.

Yes

Dependent Information

Specifically identify the personal information collected, and describe the intended use of the information.

Veterans' dependant data, including name, relation to veteran, and SSN will be utilized to determine eligibility for VA

benefits.

Yes

Service Information

Specifically identify the personal information collected, and describe the intended use of the information.

Service information data will be utilized to identify veterans and determine eligibility for level benefits to be received.

Yes

Medical Information

Specifically identify the personal information collected, and describe the intended use of the information.

Medical data such as disability information regarding a veteran will be utilized to provide improved quality healthcare and support more targeted benefits information to be provided to veterans and their dependants.

No

Criminal Record Information

Specifically identify the personal information collected, and describe the intended use of the information.

Yes

Guardian Information

Specifically identify the personal information collected, and describe the intended use of the information.

Veterans' guardian information including name, relationship to veteran, and SSN, will be utilized to determine eligibility for VA benefits.

Yes

Education Information

Specifically identify the personal information collected, and describe the intended use of the information.

Veterans' education information, including education level and graduation date will be utilized to determine eligibility for VA benefits.

Yes	Rehabilitation Information
-----	-----------------------------------

Specifically identify the personal information collected, and describe the intended use of the information.

Medical data including rehabilitation and disability information regarding a veteran will be utilized to provide improved quality healthcare and support more targeted benefits information to be provided to veterans and their dependants.

No	Other Personal Information (specify):
----	--

The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.2 Data Sources	
<i>Identify the source(s) of the collected information.</i>	
a) Select all applicable data source categories provided below.	
b) For each category selected:	
i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.	
Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)	
Note: PIV projects should use the "Other Source(s)" data source.	
Yes	Veteran Source
No	Public Source(s)

i) Specifically identify the Public Source(s) - identify the specific organization(s) or other entity(ies) that supply personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

Yes

VA Files and Databases

i) Specifically identify each VA File and/or Database that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

This project will connect to existing VA files and databases including BDN, VBA Corporate Database, VISTA, AAC and VA medical centers to continuously update veteran records and will serve as the ultimate, authoritative source of veteran id data.

Yes

Other Federal Agency Source(s)

i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

This project intends to utilize veteran data from NOAA, Coast Guard, DEERS and DIMHRS to provide the most up-to-date veteran id data and assist with eligibility determination.

No

State Agency Source(s)

i) Specifically identify each State Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No

Local Agency Source(s)

i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No	Other Source(s)
----	-----------------

i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.3 Collection Methods

Identify and describe how personal information is collected:

a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.

Yes	Web Forms:	Information collected on Web Forms and sent electronically over the Internet to project systems.
-----	-------------------	--

Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")

Web site(s) and portals for this project are currently in the requirements/planning phase and URL's have yet to be assigned.

Yes	Paper Forms:	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.
-----	---------------------	--

Identify and/or describe the paper forms by which data is collected. If applicable, identify standard VA forms by form number.

This project is in the requirements definition phase and business needs are being identified and data collection forms have not yet been finalized.

Yes	Electronic File Transfer:	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.
-----	----------------------------------	--

Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection – how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)

Data feeds from veteran data from NOAA, Coast Guard, DEERS and DIMHRS will be used for outreach and to verify

Veteran data.

Yes	Computer Transfer Device:	Information that is entered and/or stored on one computer/ system and then transferred to project IT systems via an object
		or device that is used to store data, such as a CD-ROM, floppy disk or tape.

Describe the type of computer transfer device, and the process used to collect information.

A critical piece of the CM project is the interface with the DoD's DEERS and DMDC data feeds including G2C, C2G, G2B, VA2VA data flows.

Yes	Telephone Contact:	Information is collected via telephone.
-----	---------------------------	---

Describe the process through which information is collected via telephone contacts.

The CM project will utilize a web-enabled telephony solution that has not been fully defined nor developed.

Yes	Other Collection Method:	Information is collected through a method other than those listed above.
-----	---------------------------------	--

If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.

Medium for collecting information has not been developed fully at this time.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.4 Notice

The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?

Yes

Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.

5.4.b) Is the data collection mandatory or voluntary?

Voluntary

5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?

The procedures to notify individuals of the Privacy Policy will be in compliance and agreement with the Privacy Act of 1974 and VA policy and are in process of being determined and documented.

5.4.d) Is the data collection new or ongoing?

Ongoing

5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)

	Not applicable
Yes	Privacy notice is provided on each page of the application.
Yes	A link to the VA Website Privacy Policy is provided.
Yes	Proximity and Timing: the notice is provided at the time and point of data collection.
Yes	Purpose: notice describes the principal purpose(s) for which the information will be used.
Yes	Authority: notice specifies the legal authority that allows the information to be collected.
Yes	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.
Yes	Disclosures: notice specifies routine use(s) that may be made of the information.

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:

The Privacy Notices for this project are currently under development.

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

Yes

Web Forms:

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The project is still under development, however, notification of privacy will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

Yes

Paper Forms:

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The project is still under development, however, notification of privacy will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

Yes

Electronic File Transfer:

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

The project is still under development, however. the project will abide by VA and Federal rules and directives regarding the sharing/encrypting of information.

Yes

Computer Transfer Device:

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

The project is still under development, however, notification of privacy will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

Yes

Telephone:

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The project is still under development, however, notification of privacy will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

Yes

Other Method:

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The project is still under development, however, notification of privacy will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.5 Consent For Secondary Use of PII:

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

5.5.a) Will personally identifiable information be used for any secondary purpose?

Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."

No

5.5.b) Describe and justify any secondary uses of personal information.

5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

Some examples of consent methods are: (1) Approved OMB consent forms and (2) VA Consent Form (VA Form 1010EZ). Provide justification if no method of consent is provided.

	Web Forms:
--	-------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

The project is still under development, however, collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the project will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

	Paper Forms:
--	---------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

The project is still under development, however, collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the project will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

	Electronic File Transfer:
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	Computer Transfer Device:
<p><i>For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:</i></p> <p><i>a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.</i></p> <p>The project is still under development, however, collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the project will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.</p>	
	Telephone Contact Media:
<p><i>Describe:</i></p> <p><i>1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.</i></p> <p>The project is still under development, however, collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the project will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.</p>	
	Other Media
<p><i>Describe:</i></p> <p><i>1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.</i></p> <p>The project is still under development, however, collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the project will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.</p> <p><i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i></p>	

5.6 Data Quality
<p><i>5.6.a) Explain how collected data are limited to required elements:</i></p> <p>This project will follow VA guidelines and will comply with federal regulatory requirements to develop appropriate data collection procedures and safeguard veteran id data.</p>
<p><i>5.6.b) How is data checked for completeness?</i></p>

The project will develop criteria to flag potentially incomplete data and will assign responsibilities to check completeness of the "flagged" data.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?

The specific steps and procedures to ensure data integrity and completeness have not yet been developed. However, part of the project is designed to verify the data for relevance, authenticity and accuracy prior to becoming part of the system. The project plans to utilize time stamps for critical records and procedures will be developed to update veterans' data when contact is made with veterans.

5.6.d) How is new data verified for relevance, authenticity and accuracy?

The specific steps and procedures to ensure data relevancy, integrity and completeness have not yet been developed. However, part of the project is designed to verify the data for relevance, authenticity and accuracy prior to becoming part of the system.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIA 2008 SECTIONS 6 - 13

Project Name

One VA Contact Management-2008

6. Use and Disclosure

6.1 User Access and Data Sharing

Identify the individuals and organizations that have access to system data.

--> *Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.*

--> *Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.*

--> *Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.*

6.1.a) *Identify all individuals and organizations that will have access to collected information. Select all applicable items below.*

Yes

System Users

Yes

System Owner, Project Manager

Yes

System Administrator

No

Contractor

If contractors to VA have access to the system, describe their role and the extent of access that is granted to them. Also, identify the contract(s) that they operate under.

Yes

Internal Sharing: Veteran Organization

If information is shared internally, with other VA organizations identify the organization(s). For each organization, identify the information that is shared and for what purpose.

Organizations include VBA, VHA and NCA (systems to be affected include VHA Common Services and Vista, VBA Corporate applications including VETSNET, and others) and the information shared with all of these organizations includes Veteran personal identification data, military history, disability data.

Yes

Other Veteran Organization

If information is shared with a Veteran organization other than VA, identify the organization(s). For each organization, identify the information that is shared and for what purpose.

Yes

Other Federal Government Agency

If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

Social Security Administration, IRS, Department of Defense, personal Veteran ID data to verify Veteran ID data and update Veteran data.

No

State Government Agency

If information is shared with a State government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

No

Local Government Agency

If information is shared with a local government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

Yes

Other Project/ System

If information is shared with other projects or systems:

1) Identify the other projects and/or systems, and briefly describe the data sharing. 2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system. 3) For each project and/or system with which information will be shared, describe why information is shared. 4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.

TBD, data sharing/access still under development as part of requirements definition but will comply with OMB and VA

directives regarding privacy and data security.

No

Other User(s)

If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:

Users include VA employees who deliver benefits to veterans., system management and support, management, and maintenance functions will have access to the personal information. Procedures to detect and deter browsing and unauthorized access will be defined when the project moves to deployment or operational phase. The project plans to share the collected personal information with DoD and other authorized partners. Within VA, the new project potentially will share data with VA financial management system, BDN, VBA Corporate Database, VistA, VHA Health Data Repository (HDR). However, the exact systems to share data with and the control methods to ensure that only defined data are transmitted are not defined yet.

6.1.b) How is access to the data determined?

Access to the data will be role-based, specifically to limit access to the least amount necessary to perform the VA's normal duties and provide service to the veteran.

6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.

The exact criteria, procedures, controls and responsibilities regarding access will be defined and documented at a later stage in the project.

6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.

User access will be restricted based on job function.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

The CM project will utilize the existing privacy training that is already available to VA employees and business partners including training materials and privacy processes and guidelines to safeguard veteran id data and prevent misuse. These training materials and processes will be documented and provided to all relevant users and will be monitored closely.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

Yes

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

Measures are still under development but will comply with OMB and VA directives regarding privacy and data security.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.

Every system, system user, partner will share responsibility for protecting the privacy rights of individuals and the VA's privacy rights policy will be strictly enforced.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.

Data sharing will undergo encryption process and will abide by strict OMB and VA data policies.

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

MOU currently in place with Department of Defense and reflects the scope of the information currently shared.

6.1.k) How is the shared information secured by the recipient?

Data will be encrypted.

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?

This project is still in development phase, training to be determined.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

6.2 Access to Records and Requests for Corrections

The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.

6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by VA? (Select all applicable options below.)

Yes	The application will provide a link that leads to their information.
Yes	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
Yes	The application will provide a phone number of a VA representative who will provide instructions.
Yes	The application will use other method (explain below).
	The application is exempt from needing to provide access.

6.2.b) What are the procedures that allow individuals to gain access to their own information?

These procedures are currently under development.

6.2.c) What are the procedures for correcting erroneous information?

These procedures are currently under development.

6.2.d) If no redress is provided, are alternatives available?

These procedures are currently under development.

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

The project is still under development, however, access to records and requests for collection will be determined and documented as Standard Operating Procedures and will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

7 Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

System of Records Notices may be accessed via:

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

or

http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html

For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.

VHA Handbook 1907.1 may be accessed at:

http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434

For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.

Start by looking at the <http://www.warms.vba.va.gov/20rcs.html>

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

CM will not "own" any data, it will use data provided by other VA systems and efforts.

7.b) What are the procedures for eliminating data at the end of the retention period?

N/A

7.c) Where are procedures documented?

N/A

7.d) How are data retention procedures enforced?

N/A

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:

Risk-based security monitoring, testing and evaluation will be conducted on a regular basis.

8.1.c) Is adequate physical security in place to protect against unauthorized access?

Yes

8.2 Project-Specific Security Measures

8.2.a) Provide a specific description of how collected information will be secured.

- A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.
- A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).
- A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.
- Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? If so, describe these controls.

CM will use the data in other systems (VADIR, VA Corp DB, VHA, etc). The security will be addressed at those systems – the CM applications will integrate with VA security services. Management, operational and technical controls will be in place to ensure data security. All controls will be detailed in the System Security Plan. All security controls are implemented through a cohesive security structure and is geared to mitigating risk to information and information resources to acceptable levels. In addition to risk management, other management level controls such as system security planning, certification and accreditation and security reviews are also implemented to assure that controls reflect management policies at operational levels including at the enterprise, business line and project level. Operational and technical controls such as contingency planning input/output setting, data integrity and validation measures and logical access control are implemented on the various network, system, server and application levels to assure that information is secured in transit, process and storage. For example, the VA employs a virtual private network to assure the privacy of information in transit. This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. System interconnection agreement (SIA)s are a system level measure to ensure that all interconnected systems meet minimum VA access policies for interconnected systems from within and outside the VA wide area network (WAN) boundaries. Moreover, the VA employs a comprehensive incidence response unit to respond to unwanted incursions and institutes enterprise level anti-virus system to protect mission critical applications on the desktop. Finally, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

CM follows VA policy, procedures, and guidance to ensure it complies with Federal law including the E-Government Act of 2002, FISMA, and the Privacy Act.

9. CHANGE RECORD

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, n/a: first PIA)

No

If no, then proceed to Section 10, "Children's Online Privacy Protection Act."

If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

- For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

- For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);

List All Major Project/System Modification(s)	State Justification for Modification(s)	*Concisely describe:	Modification Approver	Date

10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT
10.a) Will information be collected through the Internet from children under age 13?
No
If "No" then SKIP to Section 11, "PIA Considerations".
10.b) How will parental or guardian approval be obtained.
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

11. PIA CONSIDERATIONS
11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.
As a result of performing the PIA, emphasis and attention to the PIA requirements will be applied to preparing a data quality management plan, addressing security and privacy concerns including ensuring that collection of personal information contains appropriate consent and release information and developing comprehensive standard operating procedures (SOP). The PIA also provided an opportunity to review Privacy Act System of Records Notices and ensure the appropriate notices are in place before going operational.
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:
13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the development time and cost of this project and must be planned for accordingly. I will ensure that VA privacy and information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.
Yes
13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)
Rebecca Wells, 08/22/2006
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)